IN THE UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF ALABAMA
NORTHERN DIVISION

UNITED STATES OF AMERICA	)	
	)	
v.	)	CASE NO. 2:17-CM-3152-WC
	)	[WO]
IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH FIFTEEN EMAIL ADDRESSES STORED AT PREMISES OWNED, MAINTAINED, CONTROLLED OR OPERATED BY 1&1 MEDIA, INC., GOOGLE, INC., MICROSOFT5 CORP. and YAHOO! INC.	)	

MEMORANDUM OPINION

On June 15, 2017, the Government submitted fifteen separate search warrant applications to the Magistrate Judge. The applications were all part of the same investigation of tax fraud and identity theft, and they all wanted disclosure of the same thing: everything—all information, all emails, all usage history, everything—related to fifteen email accounts maintained by different electronic communications service providers. The Magistrate Judge denied the applications. *In re Search of Information Associated With Fifteen Email Addresses*, No. 2:17-CM-3152-WC, 2017 WL 3055518 (M.D. Ala. Jul. 14, 2017); (Doc. # 1, at 13.) The Government now seeks review. (Doc. # 2.)

I. BACKGROUND

A. The Warrant Applications

The fifteen applications the Government submitted all relate to a multi-year investigation of a multi-million-dollar scheme to defraud using stolen identities. The applications were filed under seal, and those particular facts need not be recited here. Suffice it to say that certain email accounts the Government had already searched contained emails sent to or received from the new accounts that contained information of the sort the Government was investigating. The Government applied to the Magistrate Judge with these additional warrant applications to require the third-party electronic communications service providers—the hosts of the email accounts—to turn over all the information associated with the accounts.

Each of the warrant applications consisted of two attachments. Attachment A described the thing or property to be searched—here, the specific email account and its provider. Attachment B described the "Particular Items to be Seized." This section was then divided into (1) the "Information to be disclosed" by the provider, and (2) the "Information to be seized by the Government."

As the "Information to be disclosed," the Government sought:

> a. The contents of all e-mails associated with the account, including stored or preserved copies of e-mails sent to and from the account, draft emails, the source and destination addresses associated

> with each e-mail, the date and time at which each e-mail was sent, and the size and length of each e-mail;
> b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);
> c. The types of service utilized;
> d. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;
> e. All records pertaining to communications between [the provider] and any person regarding the account, including contacts with support services and records of actions taken.
> f. All location data associated with the account.
> g. All location history associated with the account, whether derived from Global Positioning System (GPS) data, cell site/cell tower triangulation/trilateration, and precision measurement information such as timing advance or per call measurement data, and Wi-Fi location. Such data shall include the GPS coordinates and the dates and times of all location recordings.
> h. All identity and contact information, including full name, e-mail address, physical address (including city, state, and zip code), date of birth, phone numbers, gender, hometown, occupation, and other personal identifiers.

(*E.g.*, Doc. # 1-1, at 5–6.[1]) According to Attachment B's Section 2, though all of the above information would be "disclosed," only the following components would be "seized":

[1] Though the Government submitted fifteen separate applications, Attachments A and B were identical throughout except for the name of the specific provider.

All information described above in Section 1 that constitutes fruits, evidence and instrumentalities of violations of Title 18, United States Code, Section 1028A [Identity Theft]; Title 18, United States Code, Section 1030 [Computer-related Fraud]; and title 18, United States Code, Section 1343 [Fraud by Wire, Radio, or Television] since January 1, 2015, including information pertaining to:

a. Records and communications regarding the transmission of personally identifiable information, IRS Forms W-2, tax returns, prepaid debit cards, the proceeds of the transfer or use of personally identifiable information, and a conspiracy to file false tax returns using stolen identities;
b. Records and communications regarding any property derived from the proceeds of the conspiracy;
c. Records relating to who created, used, or communicated with the account or identifier, including records about their identities and whereabouts; and
d. Records indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner, including all geolocation information.
e. Records relating to the identities of the person(s) who communicated with the user ID about matters described in paragraph 2.a., including records that help reveal their whereabouts.

(Doc. # 1-1, at 6.)

Finally, the affiant also described how the warrant would be executed:

I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A), by using the warrant to require [the provider] to disclose to the government copies of the records and other information (including the content of communications) particularly described in Attachment A and Section 1 of Attachment B. Upon receipt of the information described in Section 1 of Attachment B, government-authorized persons will review that

> information to locate the items described in Section 2 of Attachment B.

(Doc. # 1-1, at 18.)

B. The Magistrate Judge's Ruling

The Magistrate Judge denied the Government's applications. In doing so, the Magistrate Judge explained two specific problems with the proposed warrant. First, he found that "the Government's collection of data [was] not temporally limited despite its temporally-limited showing of probable cause (and its manifest intent to only seize evidence of specific crimes 'since January 1, 2015')." Second, he was concerned "that the Government w[ould] keep and retain access indefinitely to all nonpertinent data it receives." (Doc. # 1, at 6.) That is, since there were not "any protocol[s] for the Government's handling of non-pertinent information that the Government would compel the [providers] to disclose but that it ostensibly [would] not 'seize,'" the Government would be able to keep indefinitely someone's personal information that, by the Government's own determination, did not relate to the object of the search. (Doc. # 1, at 12.)

The Magistrate Judge also elaborated on his general discomfort with the broad nature of searches conducted under the seize-first, search-second protocol of Federal Rule of Criminal Procedure 41(e)(2)(B).[2] In his view, the premise "that

[2] "A warrant . . . may authorize the seizure of electronic storage media or the seizure or copying of electronically stored information. Unless otherwise specified, the warrant authorizes

there is a distinction between what is disclosed to, and apparently kept by, the Government, and what the Government actually 'seizes,'" is false. (Doc. # 1, at 6–7.) Accordingly, the Magistrate Judge found that the "disclosure"—read "seizure"—of all of the email accounts here would be unreasonable. (Doc. # 1, at 9–10.)

II. JURISDICTION

Warrants sought pursuant to the Stored Communications Act of 1986, such as those here, may be issued "using the procedures described in the Federal Rules of Criminal Procedure . . . by a court of competent jurisdiction." 18 U.S.C. § 2703(a), (b)(1)(A), (c)(1)(A). A court of competent jurisdiction is "any district court of the United States (including a magistrate judge of such a court)" that, inter alia, has jurisdiction over the offense being investigated. *Id.* § 2711(3)(A). Since the offenses being investigated here are aggravated identity theft under 18 U.S.C. §§ 1028A, 1030, and 1343, jurisdiction is proper. *See* 18 U.S.C. § 3231.

III. STANDARD OF REVIEW

Review of the Magistrate Judge's order denying the Government's application for a search warrant is governed by the Federal Magistrates Act, 28

---

a later review of the media or information consistent with the warrant. The time for executing the warrant in Rule 41(e)(2)(A) [requiring the warrant to be executed "within a specified time no longer than 14 days"] . . . refers to the seizure or on-site copying of the media or information, and not to any later off-site copying or review." Fed. R. Crim. P. 41(e)(2)(B).

U.S.C. § 631 *et seq*. Because search warrants are included in the criminal pretrial matters appropriately handled by magistrate judges, *see Gomez v. United States*, 490 U.S. 858, 868 n.16 (1989), the denial of the warrants will be reviewed under the clearly erroneous standard. *See* 28 U.S.C. § 636(b)(1)(A). "A finding is 'clearly erroneous' when[,] although there is evidence to support it, the reviewing court on the entire evidence is left with the definite and firm conviction that a mistake has been committed." *United States v. U.S. Gypsum Co.*, 333 U.S. 364, 395 (1948).

IV. DISCUSSION

A. General Warrant Requirements

The Fourth Amendment provides that "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV. This is typically broken down into three requirements: (1) a neutral magistrate, (2) probable cause, and (3) particularity. *See Dalia v. United States*, 441 U.S. 238, 255 (1979). If these requirements are met, a judge "must issue the warrant." Fed. R. Crim. P. 41(d)(2).

The mandatory nature of Rule 41's conditional statement seems to leave little (if any) discretion to the judge in shaping how the search itself must be exercised. There is some tension, then, between this rule and the increasingly

common practice of judges requiring *ex ante* that additional safeguards be added to warrants in the digital context. For instance, in a concurring opinion to an en banc Ninth Circuit case, Chief Judge Kozinski advised magistrate judges to require five additional limitations on search warrants of electronically stored data. *See United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1178–80 (9th Cir. 2010) (en banc) (Kozinski, J., concurring). He suggested judges: (1) insist that the Government waive reliance on the plain view doctrine; (2) require either a third party or an independent search team to conduct the initial search and segregation of the data and hand over only the information that is the target of the warrant to the investigative team; (3) disclose in the warrant the risks of destruction of information; (4) insist that the Government hew closely to search protocols designed to uncover only the information for which it has probable cause; and (5) require the Government to destroy or return the non-responsive data. *Id.* at 1180.

At least some lower courts have taken the advice and required certain *ex ante* restrictions to the Government's proposed search.[3] *E.g.*, *In re the Search of Premises Known as: Three Hotmail Email Accounts*, No. 16-MJ-8036-DJW, 2016

[3] Others have not. *E.g.*, *United States v. Galpin*, 720 F.3d 436, 451 (2d Cir. 2013) ("Unlike the Ninth Circuit, we have not required specific search protocols or minimization undertakings as basic predicates for upholding digital search warrants."); *United States v. Stabile*, 633 F.3d 219, 241 n.16 (3d Cir. 2011) (declining "to follow the Ninth Circuit's suggestion to 'forswear reliance on the plain view doctrine'"); *United States v. Mann*, 592 F.3d 779, 785 (7th Cir. 2010) ("We are . . . skeptical of a rule requiring officers to always obtain pre-approval from a magistrate judge to use the electronic tools to conduct searches tailored to uncovering evidence that is responsive to a properly circumscribed warrant.").

WL 1239916, at *18–23 (D. Kan. Mar. 28, 2016), *rev'd in part*, 212 F. Supp. 3d 1023; *In re the Search of Information Associated with [redacted]@mac.com*, 25 F. Supp. 3d 1, 7–9 (D.D.C. 2014), *vacated*, 13 F. Supp. 3d 157; *In re [REDACTED]@gmail.com*, 62 F. Supp. 3d 1100, 1103–04 (N.D. Cal. 2014).

And the *ex ante* practice is understandable. Federal Rule of Criminal Procedure 41(e)(2)(b) authorizes the seize-first, search-second scheme that, when the initial seizure is broad, may remind courts of the "general, exploratory rummaging in a person's belongings" the Fourth Amendment was designed to prohibit. *Coolidge v. New Hampshire*, 403 U.S. 433, 467 (1971). This is true especially if the Government can keep indefinitely all the information that was initially disclosed to then search through again at a later time. *Cf. United States v. Ganias*, 824 F.3d 199, 225–26 (2d Cir. 2016) (en banc) (affirming on good-faith grounds that evidence collected from a search pursuant to a warrant in 2006 of a copy made of defendant's hard drive in 2003 was admissible, even though the probable cause for the initial warrant was for a different criminal investigation).

But there is, at least in theory, a distinction between the *ex post* review a court engages in to determine whether a search was reasonable and the *ex ante* query of whether the Government has met the probable cause and particularity requirements such that a warrant "must issue." Were there not, the warrant itself would need to prescribe the precise procedures for officers to follow to ensure their

search will meet constitutional muster. Yet the Supreme Court has explicitly instructed that "[s]uch an interpretation is unnecessary," because "the manner in which a warrant is executed is subjected *to later review* as to its reasonableness." *Dalia*, 441 U.S. at 258 (emphasis added). So it is that in a case where the executing officers violated the restrictions a magistrate judge placed in the warrant, the Supreme Court nevertheless reviewed the officers' actions for whether they were reasonable *at the time they were performed*—and found that they were. *Richards v. Wisconsin*, 520 U.S. 385, 395–96 (1997); *see also United States v. Grubbs*, 547 U.S. 90, 99 (2006) ("The Constitution protects property owners . . . by interposing *ex ante*, the 'deliberate, impartial judgment of a judicial officer . . . between the citizen and the police,' and by providing, *ex post*, a right to suppress evidence improperly obtained." (quoting *Wong Sun v. United States*, 371 U.S. 471, 481–82 (1963)). "Deliberate impartial judgment" requires a magistrate judge's active engagement in the process *ex ante*, that is, to be more than a constitutional caricature in a predetermined process.

Such are the general contours of the role of the magistrate judge in determining whether to issue a search warrant. If the Government can show probable cause and particularity, the warrant should be issued; and as a general matter, *ex ante* restrictions that go beyond these requirements are disfavored, advisory in their effect, and certainly not required. *See United States v. Khanani*,

502 F.3d 1281, 1290–91 (11th Cir. 2007) (explaining that a warrant "violates the Fourth Amendment if it fails to specify the place to be searched and the items to be seized . . . or if it is not supported by probable cause," and refusing to suppress evidence recovered from a computer search where there was no written search protocol included in the warrant (citation omitted)).

B. Particularity Requirements

Turning to the Magistrate Judge's denial of the warrant applications here, at least two of the three Fourth Amendment requirements are met. There is no dispute there was a neutral magistrate. Nor is there doubt the Government showed that search of the email accounts would "aid in a particular apprehension or conviction for a particular offense," *Dalia*, 441 U.S. at 255 (citation omitted), or that "there is a fair probability that contraband or evidence of a crime will be found" in them, *Illinois v. Gates*, 462 U.S. 213, 238 (1983). (*See* Doc. # 1, at 9.) The issue is particularity.

There is no "general 'particularity requirement.'" *Grubbs*, 547 U.S. at 98. Rather, the Fourth Amendment requires only that (1) "the place to be searched" and (2) "the persons or things to be seized" be "particularly describ[ed]." *Id.* (quoting U.S. Const. amend. IV). And though the Supreme Court has described the level of particularity as such that "nothing is left to the discretion of the officer executing the warrant," *Marron v. United States*, 275 U.S. 192, 196 (1927), the

rule is generally more flexible than that. *See United States v. Wuagneaux*, 683 F.2d 1343, 1349 n.4 (11th Cir. 1982) (explaining that if the *Marron* statement "were construed as a literal command, no search would be possible"). Instead, "a description is sufficiently particular when it enables the searcher reasonably to ascertain and identify the things to be seized." *United States v. Santarelli*, 778 F.2d 609, 614 (11th Cir. 1985). "[E]laborate specificity is unnecessary." *United States v. Betancourt*, 734 F.2d 750, 754 (11th Cir. 1984).

Moreover, the particularity requirements are applied with "a practical margin of flexibility, depending on the type of property to be seized." *Wuagneaux*, 683 F.2d at 1349. Accordingly, "a description of property will be acceptable if it is as specific as the circumstances and nature of activity under investigation permit." *Id.*

1. The Time Period to be Searched

The Eleventh Circuit has recently noted that it is "troubling" when searches of email accounts "d[o] not limit the emails sought to emails sent or received within the time of [the suspect's] suspected participation in the conspiracy." *United States v. Blake*, 868 F.3d 960, 973 n.7 (11th Cir. 2017). Other courts have likewise emphasized the importance of the time period for which the Government seeks digital information. *E.g.*, *United States v. Hanna*, 661 F.3d 271, 287 (6th Cir. 2011) (upholding search warrant that was limited to "the time period that the

evidence suggested the activity occurred"); *In re Search of Google Email Accounts*, 92 F. Supp. 3d 944, 952 (D. Alaska 2015) (denying warrant application that "would authorize the government to seize and search the *entirety* of the six Gmail accounts, even though the government has only established probable cause to look at a small number of emails within a narrow date range"); *United States v. Shah*, No. 5:13-CR-328-FL, 2015 WL 72118, at *14 (E.D.N.C. Jan. 6, 2015) (concluding search warrant was overbroad since it "offer[ed] nothing about the time frame of the offense" and instead sought all evidence "since account inception").

As the Magistrate Judge rightly emphasized, the Government's proposed warrant applications here do not have such temporal limitations. Even though they limit the "seizure" to evidence of violations occurring on or after January 1, 2015, they would allow the "search" of the email accounts from the time of their creation. True, the Government has offered to alter the applications so that the service providers would only need to produce data generated on or after January 1, 2015 (Doc. # 2, at 15), but it is not clear that even this limitation would be sufficient for all the applications. While the initial investigation began in mid-March of 2016 and related to the filing of fraudulent 2015 federal income tax returns, there is only evidence that three of the fifteen subject email accounts were involved in 2015. (Docs. # 1-6, 1-12, and 1-13.) For five of the accounts, the only

evidence of participation comes from emails sent in 2017. (Docs. # 1-3, 1-7, 1-8, 1-10, and 1-15.)

Accordingly, as detailed in the accompanying Order, though all the warrants will prohibit the disclosure of account data prior to January 1, 2015, stricter temporal limitations will be placed on a case-by-case basis. Those additional requirements will be based on an assumption that data from three months before the first activity the Government currently has evidence of, and three months after the last, would more particularly describe the time period of information to be searched. Of course, should these searches reveal more evidence of criminal activity, the Government is free to seek additional search warrants.

2. The Place to be Searched

Blake is also instructive to understanding other particularity requirements in the digital context—and why the Magistrate Judge did not clearly err in deciding the Government's applications here do not meet them. In *Blake*, the Eleventh Circuit approved a search warrant for an email account because it "limited the emails to be turned over to the government, ensuring that only those that had the potential to contain incriminating evidence would be disclosed." 868 F.3d at 973. But the court contrasted that search with one of the Facebook account, which did not "limit[] the request to [Facebook] messages sent to or from persons suspected at that time of being prostitutes or customers." *Id.* at 974. Though ultimately

resolving the issue on other grounds, the court's dicta cast doubt on the validity of the second search.

The Government argues that such particularity is not required here because of Rule 41's seize-then-search two-step procedure, which courts in other circuits have upheld. (Doc. # 2, at 10–11 (citing *United States v. Evers*, 669 F.3d 645, 652 (6th Cir. 2012); *United States v. Stabile*, 633 F.3d 219, 234 (3d Cir. 2011); *United States v. Bach*, 310 F.3d 1063, 1065 (8th Cir. 2002); *United States v. Hay*, 231 F.3d 630, 637–39 (9th Cir. 2000); and *United States v. Upham*, 168 F.3d 532, 534 (1st Cir. 1999)). But almost all the cases the Government relies on addressed the search of computers and hard drives, not email accounts. The one remaining case considered the search of emails by a third party, not by the Government. *See Bach*, 310 F.3d at 1066.

What is more, the Eleventh Circuit in *Blake* distinguished many of these exact cases from the online social media context. The court first acknowledged that "[h]ard drive searches require time-consuming electronic forensic investigation with special equipment" due to the myriad ways one can hide evidence on a hard drive. 868 F.3d at 974. "By contrast," the court explained, "when it comes to Facebook account searches, the government need only send a request with the specific data sought and Facebook will respond with precisely that data." *Id.*

Email accounts fall somewhere in the middle. Given the variety of services to enable users not only to store email but also to retain calendar information, address books, pictures, files, videos, and anything else one wants to store in the cloud, there are more ways to hide things in email accounts than on Facebook. Even so, sorting the main content—emails—by date or sender or recipient or even by keyword would be much easier than sorting data stored on a hard drive. As the DOJ's electronic search manual explains, investigators initially simply "serve the warrant on the provider as they would a subpoena, and the provider produces the material specified in the warrant." U.S. Dep't of Justice, *Searching and Seizing Computers and Electronic Evidence in Criminal Investigations* 134 (2009). This cannot be done in the more intricate, user-controlled computer context.

One way to assure particularity here, then, would be by restricting how the Government searches the email data. Of course, actually requiring the Government to submit its search protocols or methods would come dangerously close to—if not cross—the line between ensuring that warrants describe with particularity the place to be searched and creating advisory *ex ante* restrictions. Indeed, according to Professor Orin Kerr, whom the Government cites in its brief, "a particular description of how the search must be executed is neither a description of the place to be searched nor a description of the items to be seized. Instead, it is . . . a limitation on how the warrant must be executed." Orin Kerr, *Ex*

Ante Regulation of Computer Search and Seizure, 96 Va. L. Rev. 1241, 1276 (2010).

But as the Supreme Court of Vermont has persuasively explained, in the digital world, *where* an officer can search and *how* he or she goes about doing so is often indistinguishable. *See In re Search Warrant*, 71 A.3d 1158, 1170–71 (Vt. 2012).

> Even in traditional contexts, a judicial officer may restrict a search to only a portion of what was requested—a room rather than an entire house, or boxes with certain labels rather than an entire warehouse. In other words, some ex ante constraints—of the form "here, not there"—are perfectly acceptable. . . .
>
> Often the way to specify particular objects or spaces will not be by describing their physical coordinates but by describing how to locate them. This is especially true in the world of electronic information, where physical notions of particularity are metaphorical at best. . . . In the digital universe, particular information is not accessed through corridors and drawers, but through commands and queries. As a result, in many cases, the only feasible way to specify a particular "region" of the computer will be by specifying how to search.

Id.

Thus, the point is not that the Government must submit its search protocols for preapproval by the court. The Eleventh Circuit has held that such preapproval is not necessary in the computer and hard drive context. *See United States v. Bradley*, 644 F.3d 1213, 1258 (11th Cir. 2011); *Khanani*, 502 F.3d at 1290. *But see Blake*, 868 F.3d at 974 (distinguishing searches of computers and hard drives

from those of emails and social media). Rather, the point is that the Government's current request for *all* data related to *all* the email accounts is too broad. It does not describe with particularity what will be searched—or, to the extent it does, it does not establish a sufficient nexus between the place to be searched and the probable cause that would allow it. *See Warden v. Hayden*, 387 U.S. 294, 307 (1967) ("There must, of course, be a nexus . . . between the item to be seized and criminal behavior.").

With this general concern stated, some of the warrant applications are sufficiently tailored. Or, put differently, the evidence described in them is such as to allow an expansive search of the accounts. At times, "[a] warrant may be broad, in that it authorizes the government to search an identified location or object for a wide range of potentially relevant material, without violating the particularity requirement." *United States v. Ulbricht*, 858 F.3d 71, 102 (2d Cir. 2017). For instance, when there is probable cause to believe that evidence of drug activity may be found anywhere in a drug dealer's home, a search warrant authorizing a search of the entire home can be sufficiently particular. *See id.* Likewise, the Eleventh Circuit has recognized that a search of all of a business's records can be appropriate when the warrant affidavit "demonstrates a 'pattern of illegal conduct' that is likely to extend beyond the conduct already in evidence and infect the rest of the company's business." *Bradley*, 644 F.3d at 1259.

Although the proposed search warrants here are not for business records, the rule is nevertheless instructive. This is because the "pervasive fraud doctrine" or the "all records exception" is "not so much an 'exception' to the particularity requirement of the Fourth Amendment as a recognition that a warrant—no matter how broad—is, nonetheless, legitimate if its scope does not exceed the probable cause upon which it is based." *United States v. Bowen*, 689 F. Supp. 2d 675, 683 n.6 (S.D.N.Y. 2010) (citation omitted), *aff'd sub nom. United States v. Ingram*, 490 F. App'x 363, 366 (2d Cir. 2012). So it is that the *Bowen* court found that the rule applied to allow an all-records search of the personal email accounts of defendants suspected of defrauding over 100 victims of more than $5 million. *Id.* at 683. As the court reasoned, "[t]he fact that Defendants chose to use the same e-mail accounts for personal communications that they were simultaneously using to conduct their allegedly fraudulent business cannot insulate those e-mail accounts from a search pursuant to the all records exception." *Id.* at 684; *see also United States v. Falon*, 959 F.2d 1143, 1148 (1st Cir. 1992) ("[I]t would be an odd quirk in the law if, by doing fraudulent business as an individual rather than as a corporation or company, one could ensure his premises against an 'all records' search.").

Here, there are six email accounts for which the probable cause evidence is sufficiently robust to conclude that the entire email accounts from January 1, 2015,

forward can be turned over to the Government to search. (*See* Docs. # 1-4, 1-5, 1-6, 1-12, 1-13, and 1-14.) This is either because of the extended period of time for which there is evidence of criminal activity or because of the very close relationship evinced between the subject accounts and prior ones searched. As for the other accounts, as stated previously, further restrictions will be placed narrowing the time period for which the provider must turn over the account information.

For all accounts, however, the Government must restrict its search to methods or search protocols designed to uncover only information for which the Government has probable cause. To be sure, it will still be the case that, just as in the search of papers, "some innocuous documents will be examined, at least cursorily, in order to determine whether they are, in fact, among those papers [or emails] authorized to be seized." *Andresen v. Maryland*, 427 U.S. 463, 482 n.11 (1976). But in the email context, the pool of documents that must be examined can initially be narrowed in a way that paper documents in a filing cabinet cannot be. Perhaps that winnowing will occur naturally, since "Government agents generally do not manually search each and every document that is present," and instead use keyword searches that "already act[] as a 'filter' to protect innocuous information from investigators." *United States v. Sealed Search Warrant*, No. 2:17-CR-VEH-TMP-1, 2017 WL 3396441, at *2 (N.D. Ala. Aug. 8, 2017); *see also United States*

v. Deppish, 994 F. Supp. 2d 1211, 1215 (D. Kan. 2014) (approving search as reasonable where the agent "performed a filtered, keyword search" even though not specifically required to do so by the warrant). If so, then the requirement should not be burdensome, particularly since the Government need not submit those protocols for preapproval. In any event, it ensures that probable cause exists for both the place to be searched and the things to be seized. *See In re Search Warrant*, 71 A.3d at 1170–71.

C. Other Possible Restrictive Measures

As noted, some courts have encouraged the use of additional protective measures. Such limitations include requiring the search to be performed by a third party or a filter team separated from the Government's investigative team; conditioning the granting of a warrant on the Government waiving the plain view doctrine; or demanding the Government destroy or turn over the non-responsive data once searched.

As a general matter, the *ex ante* vs. *ex post* review dichotomy cautions against the imposition of additional requirements by courts issuing search warrants. *See generally* Kerr, *Ex Ante Regulation*, *supra*. Nor may a judge simply forbid investigators from seizing criminal evidence found in plain view when the Supreme Court has long said they could. *See, e.g.*, *Illinois v. Andreas*, 463 U.S. 765, 771 (1983). But it is worth emphasizing that the plain view doctrine "is

grounded on the proposition that once police are *lawfully in a position* to observe an item first-hand, its owner's privacy interest in that item is lost." *Id.* (emphasis added). Thus, to the extent the Government affirmatively searches for information outside the scope of the warrant, the plain view exception would be unavailable. *See United States v. Galpin*, 720 F.3d 436, 451 (2d Cir. 2013).

The filter team requirement is a closer question, as at least that practice has a lineage of use—though it comes usually when the Government has reason to believe that documents being searched include privileged information. *See Sealed Search Warrant*, 2017 WL 3396441, at *2 n.6 (discussing cases). But so long as the Government's search is restricted to the information for which it has presented probable cause, there is no reason here to impose segregated screening conditions. For what would doing so accomplish? "[J]ust as much private information w[ould] be exposed to the view of government strangers," and "requiring that a search be executed by one police agent versus another results in no actual limit on the search and, so, no actual protection of privacy." *In re Search Warrant*, 71 A.3d at 1188 (Burgess, J., concurring and dissenting). And so long as the plain view doctrine is not expunged (which it will not be), or the filter team gagged from passing on evidence of crimes found in plain view to the investigative team (which would amount to the same thing), there would be little, if any, difference in the practical effect of the search by the Government. *See id.*

As for provider-assisted searches, because the date range of the information to be turned over to law enforcement will be restricted, the providers will already perform the initial culling. That is a reasonable burden and one necessary to ensure particularity. But beyond this or other limited circumstances in which "the scope of the items to be seized would allow the email host to produce responsive material in a manner devoid of the exercise of skill or discretion," it would generally be unrealistic to expect Google or another email provider to conduct the search for the Government. *See In re Warrant for All Content & Other Information Associated with the Email Account xxxxxxgmail.com*, 33 F. Supp. 3d 386, 394 (S.D.N.Y. 2014); *see also Matter of Search of Information Associated with [redacted]@mac.com*, 13 F. Supp. 3d 157, 165–66 (D.D.C. 2014) (explaining that enlisting a service provider to execute the search warrant would "present nettlesome problems").

Finally, the Magistrate Judge was also concerned about what the Government would do with the data turned over by the providers but not "seized" as relevant to the investigation. (Doc. # 1, at 12.) In such a case, it would be the Government itself that determined the information it now controls is in fact outside the scope of the warrant, so it would make sense to require the Government to destroy or return that evidence. *Cf. Comprehensive Drug Testing*, 621 F.3d

at 1172 (explaining that Rule 41(g) can properly be used to "forc[e] the government to return property that it had not properly seized").

The Government argues against such a constraint. First, it contends that it would be impractical to require the destruction of non-pertinent data at the conclusion of the investigation because, by that point, "copies of the defendant's email account data might exist on a number of computer systems" and backup servers. (Doc. # 2, at 25–26.) Accordingly, "the agent who initially receives the produced data has little ability to ensure that, at the end of the case, the non-pertinent data is destroyed." (Doc. # 2, at 25.)

To be sure, while this arrangement might present practical difficulties, it would be odd indeed if the Government's own proliferation of data it itself acknowledges as outside the scope of the warrant could trump the privacy concerns protected by the Fourth Amendment merely because it would be inconvenient to undo that which it has done.

Fortunately, the issue need not be decided on this point, for the Government's other arguments are more convincing. Those are that (1) deletion of non-pertinent data could present *Brady* problems, and (2) that it might corrupt metadata associated with the package of produced data. (Doc. # 2, at 26–30.)

Brady v. Maryland, 373 U.S. 83 (1963), requires the Government to turn over any favorable evidence to the defendant that the defendant does not already

possess. *See United States v. Vallejo*, 297 F.3d 1154, 1164 (11th Cir. 2002). Although a defendant can be expected to possess data from his or her own email account, the same cannot be said for evidence recovered from the account of a co-defendant. Hence, it is conceivable that, by initially possessing and then destroying non-pertinent information, the Government could be accused of violating the requirements of *Brady*. *See Matter of Search of Information Associated with [redacted]@mac.com*, 13 F. Supp. 3d at 167 n.10 (concluding Government's *Brady* concerns "are valid").

The corruption concern is also plausible. As the Second Circuit has explained in the computer context, "digital storage media constitute coherent forensic objects with contours more complex than—and materially distinct from—file cabinets . . . [and] may need to be retained, during the course of an investigation and prosecution, to permit the accurate extraction of the primary evidentiary material sought pursuant to the warrant; to secure metadata and other probative evidence . . . ; and to preserve, authenticate, and effectively present at trial the evidence thus lawfully obtained." *Ganias*, 824 F.3d at 216. While email data already culled through and turned over by the provider may present fewer forensic problems, any import to that distinction need not be decided now. *Cf.* Brief for Google, Inc. as Amicus Curiae Supporting Defendant-Appellant, *United States v. Ganias*, 824 F.3d 199 (2d Cir. 2016) (No. 12-240-cr), 2015 WL 4597960,

at *14–16. At this time, the Government will not be required to destroy or return all the information that it possesses but does not "seize."

V. CONCLUSION

The Magistrate Judge's denial of the search warrant applications was not clearly erroneous. Because the constitutional infirmities can be corrected with moderate alterations, however, the Government's search warrants will be issued with the specific modifications described in the accompanying Order. Those limitations impose (1) a date restriction on the data to be turned over by the provider based on an individualized assessment of the accompanying probable cause evidence for each email account, and (2) an instruction applicable to all the accounts that the searches be conducted through keyword searches and other appropriate protocols so as to limit the universe of data to be reviewed to that which is more likely to be pertinent. The Government is free to return and seek additional search warrants based on the new evidence it discovers.

A separate order will be entered under seal.

DONE this 28th day of September, 2017.

/s/ W. Keith Watkins
CHIEF UNITED STATES DISTRICT JUDGE